

# UNITED STATES DISTRICT COURT

for the  
Southern District of Alabama

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

information associated with Google account  
[REDACTED]@gmail.com that is stored at premises  
controlled by Google LLC and/or Google Payment Corp

Case No. 23-MJ- 152-B

Filed under seal

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
See Attachment A (incorporated by reference).

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):  
See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):


- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 1349, 1344, 513 (a), and 1028A	Fraud conspiracy, bank fraud, possession of counterfeited or forged securities, and aggravated identity theft

The application is based on these facts:  
See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Daniel Wessel, U.S. Postal Inspector  
Printed name and title

Sworn to before me and attestation acknowledged pursuant to FRCP 4.1(b)(2).

Date: June 27, 2023

  
Judge's signature

City and state: Mobile, Alabama

Sonja F. Bivins, U.S. Magistrate Judge  
Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF ALABAMA  
SOUTHERN DIVISION

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
GOOGLE ACCOUNTS

MJ-23- 152-B

Filed Under Seal

[REDACTED] THAT IS  
STORED AT PREMISES CONTROLLED  
BY GOOGLE LLC AND/OR GOOGLE  
PAYMENT CORPORATION

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Daniel Wessel, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain Google accounts that are stored at premises owned, maintained, controlled, or operated by Google LLC and/or Google Payment Corporation ("Google"), an electronic communications service and/or remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California, as further described in Attachments A-1 through A-4, for the following accounts (collectively, the "Target Accounts"):

- a. [REDACTED]
- b. [REDACTED]
- c. [REDACTED]
- d. [REDACTED]

2. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the

SEALED

government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Postal Inspector assigned to the United States Postal Inspection Service's ("USPIS") Mobile, Alabama Domicile. In this capacity, I am responsible for investigating criminal activity related to the United States Postal Service in Mississippi and Alabama. I have been a Postal Inspector since April 2021. Prior to becoming a Postal Inspector, I was employed as a Special Agent with the United States Naval Criminal Investigative Service since September 2015. I have received training at the Federal Law Enforcement Training Center in criminal investigations and financial crimes. I have a certificate in Forensic Accounting from Georgetown University and have been a Certified Fraud Examiner since 2012. In the course of my training and experience, I have worked on numerous investigations involving fraud. Pursuant to my duties as a Postal Inspector, I have gained experience in investigations of bank fraud pertaining to the theft and counterfeiting of checks. I have participated in search and seizure operations dealing with these types of criminal offenses. I have previously written, served, and reviewed the contents of the contents of an account operated by Google LLC after obtaining the contents via a search warrant related to altered and counterfeit checks. I have submitted a preservation letter to Google requesting the preservation of data for the **Target Accounts** and I have received confirmation of that request from Google.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. All dates, times, amounts, and locations referenced in my affidavit are approximations.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1349 (fraud conspiracy), 1344 (bank fraud), 513(a) (possession of counterfeited or forged securities), and 1028A (aggravated identity theft) have been committed by [REDACTED] r [REDACTED], and others, both known and unknown. There is also probable cause to search the information described in Attachment A-1 through A-4 for evidence, instrumentalities, contraband, or fruits of these crimes further described in Attachment B.

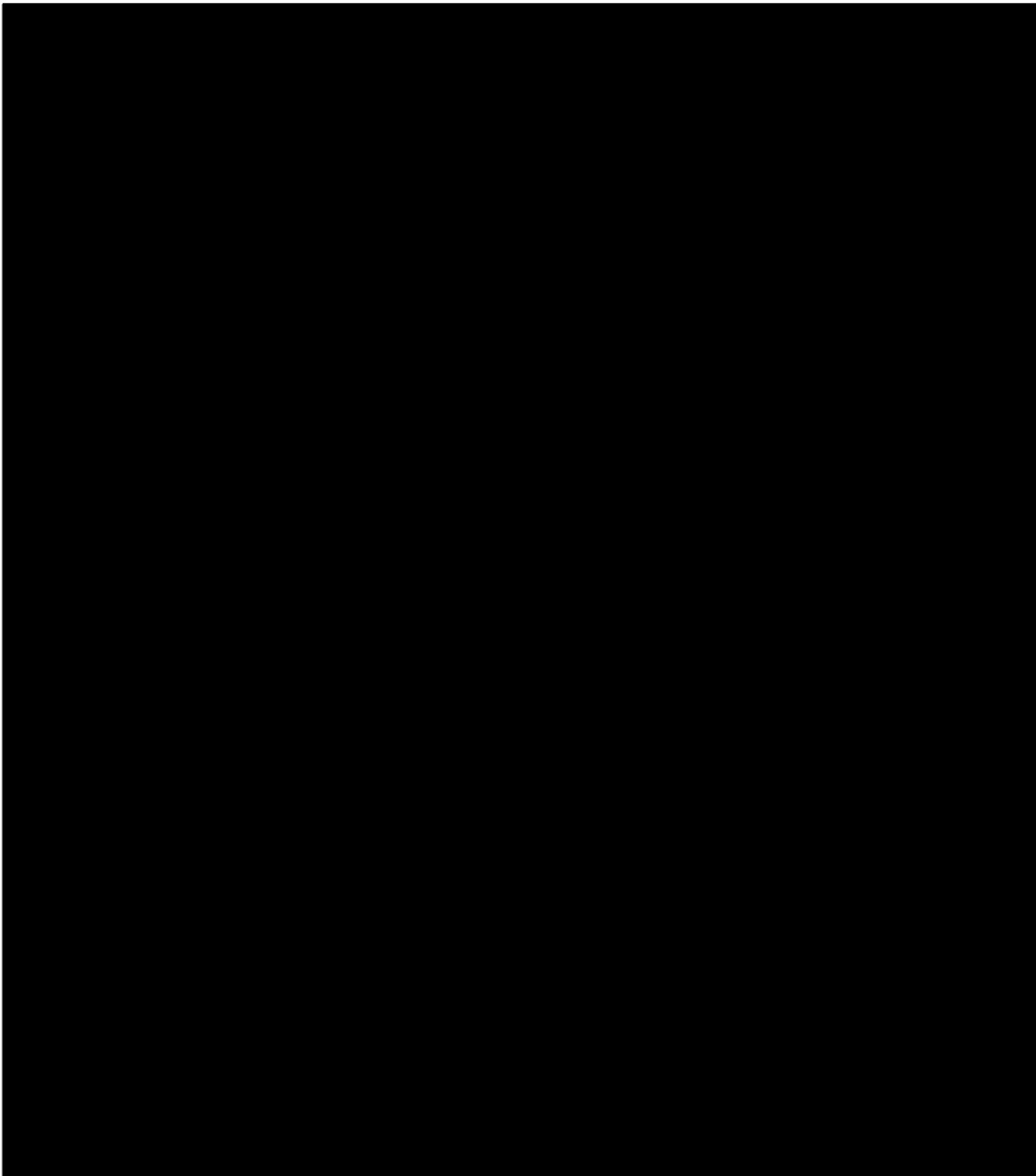
### **JURISDICTION**

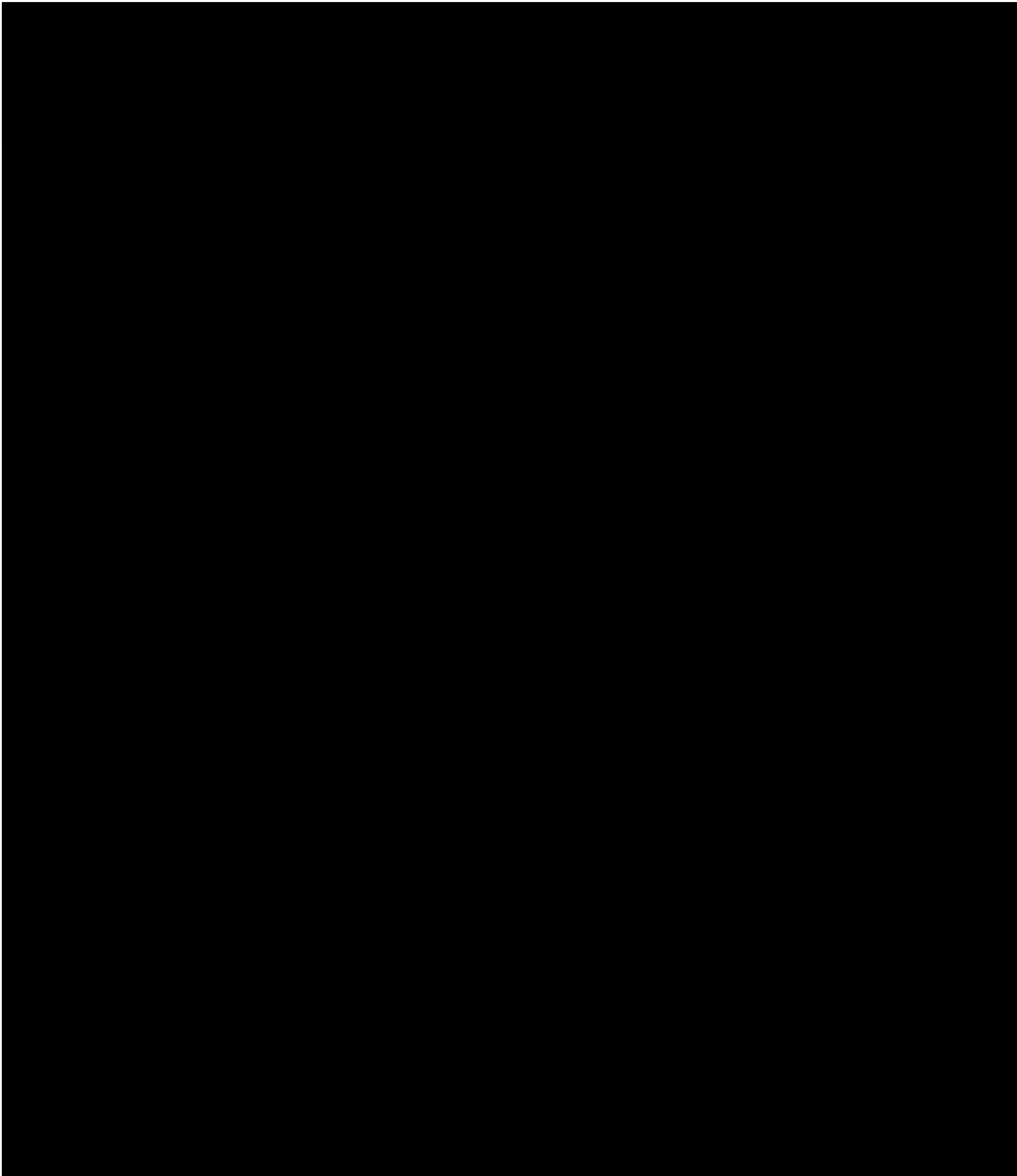
6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.”

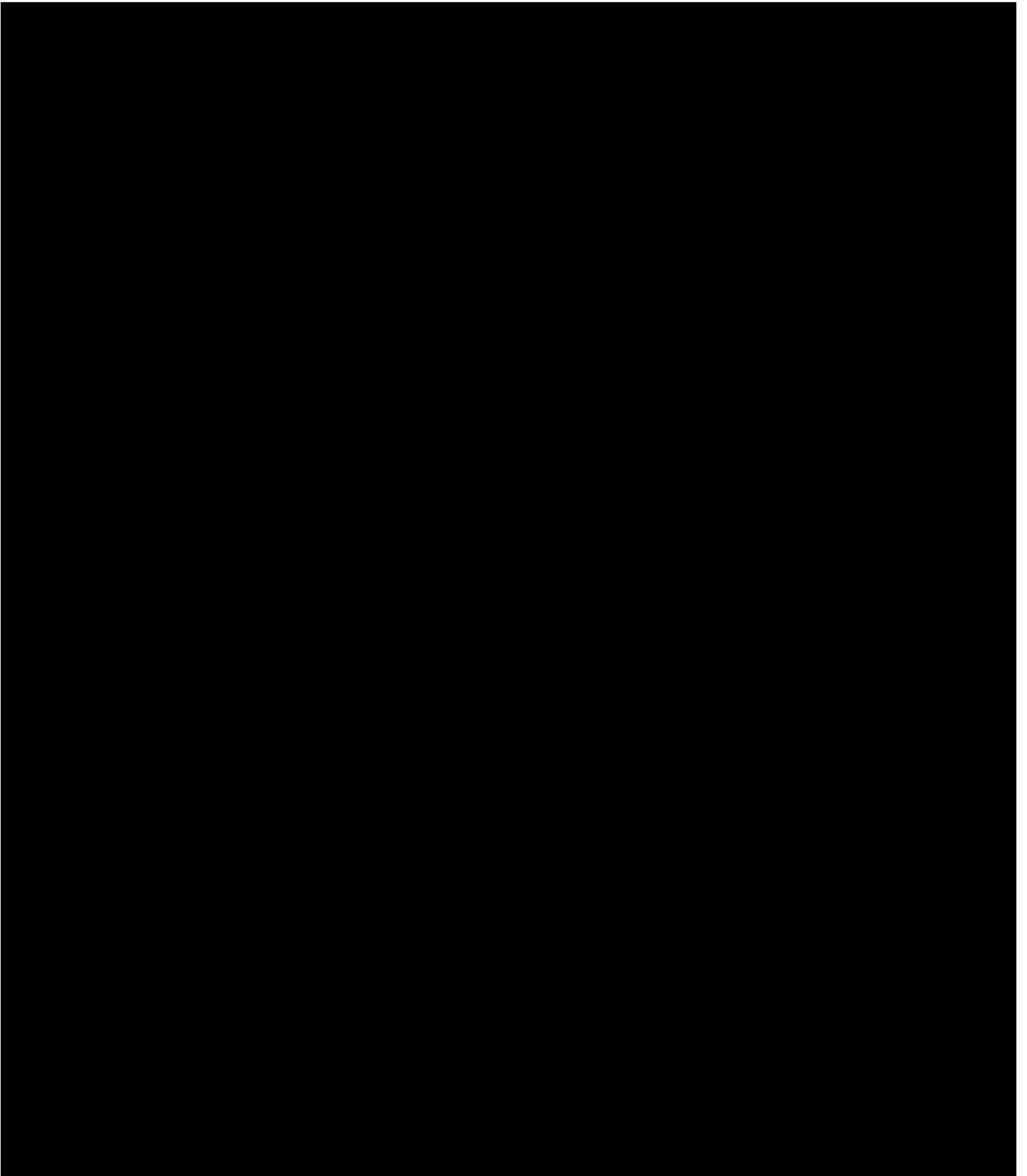
### **PROBABLE CAUSE**

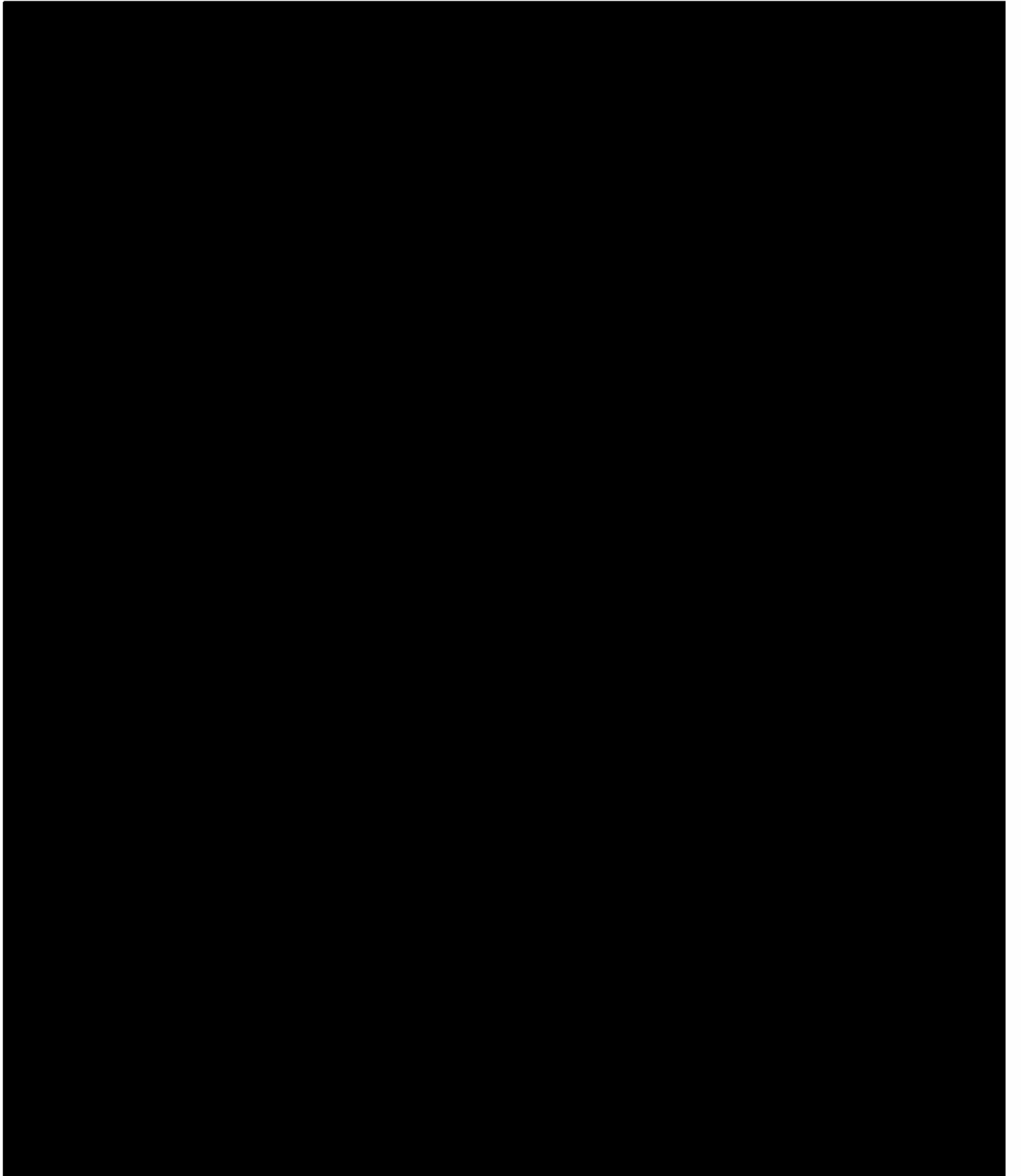
#### *The Scheme*



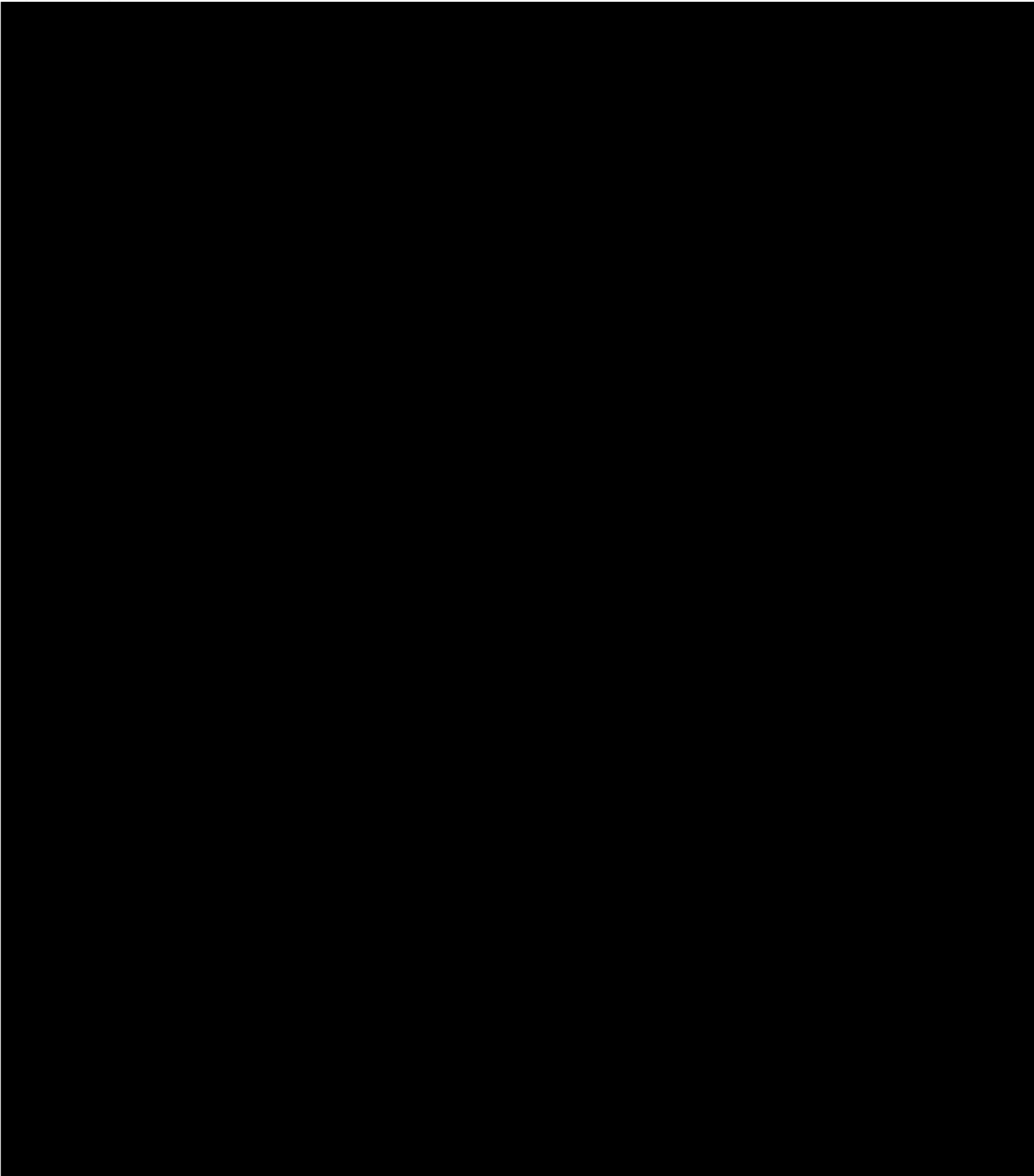


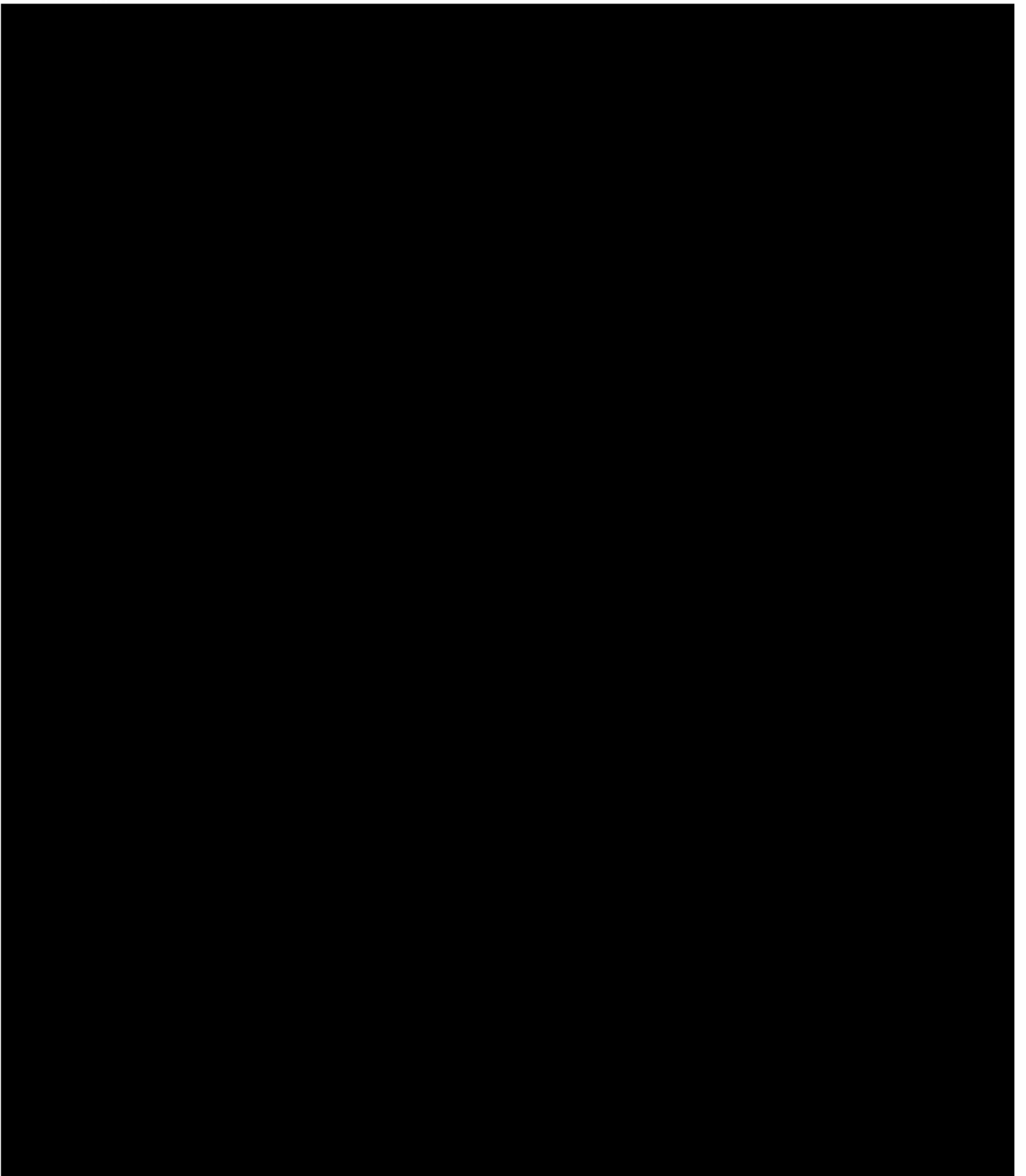


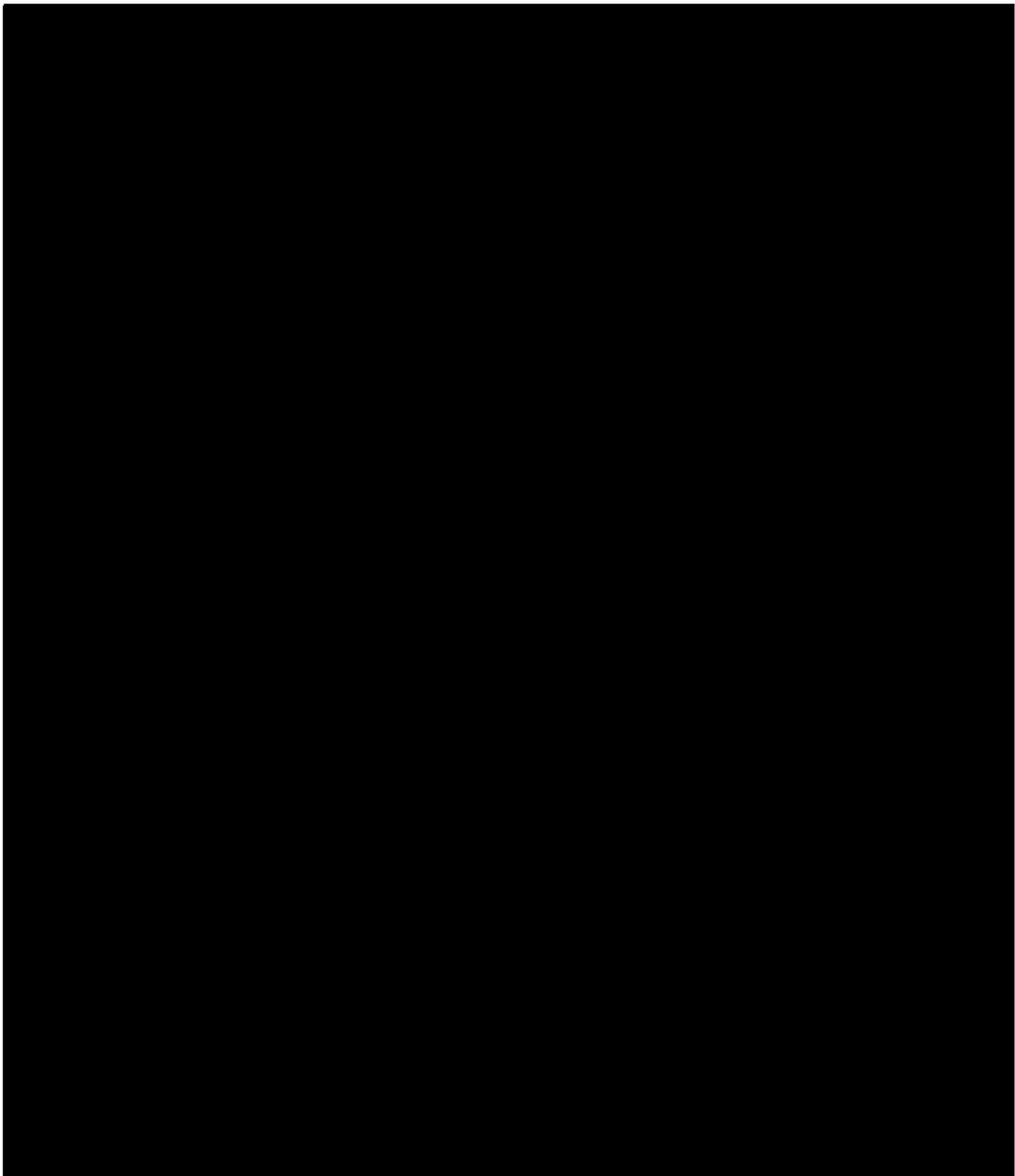


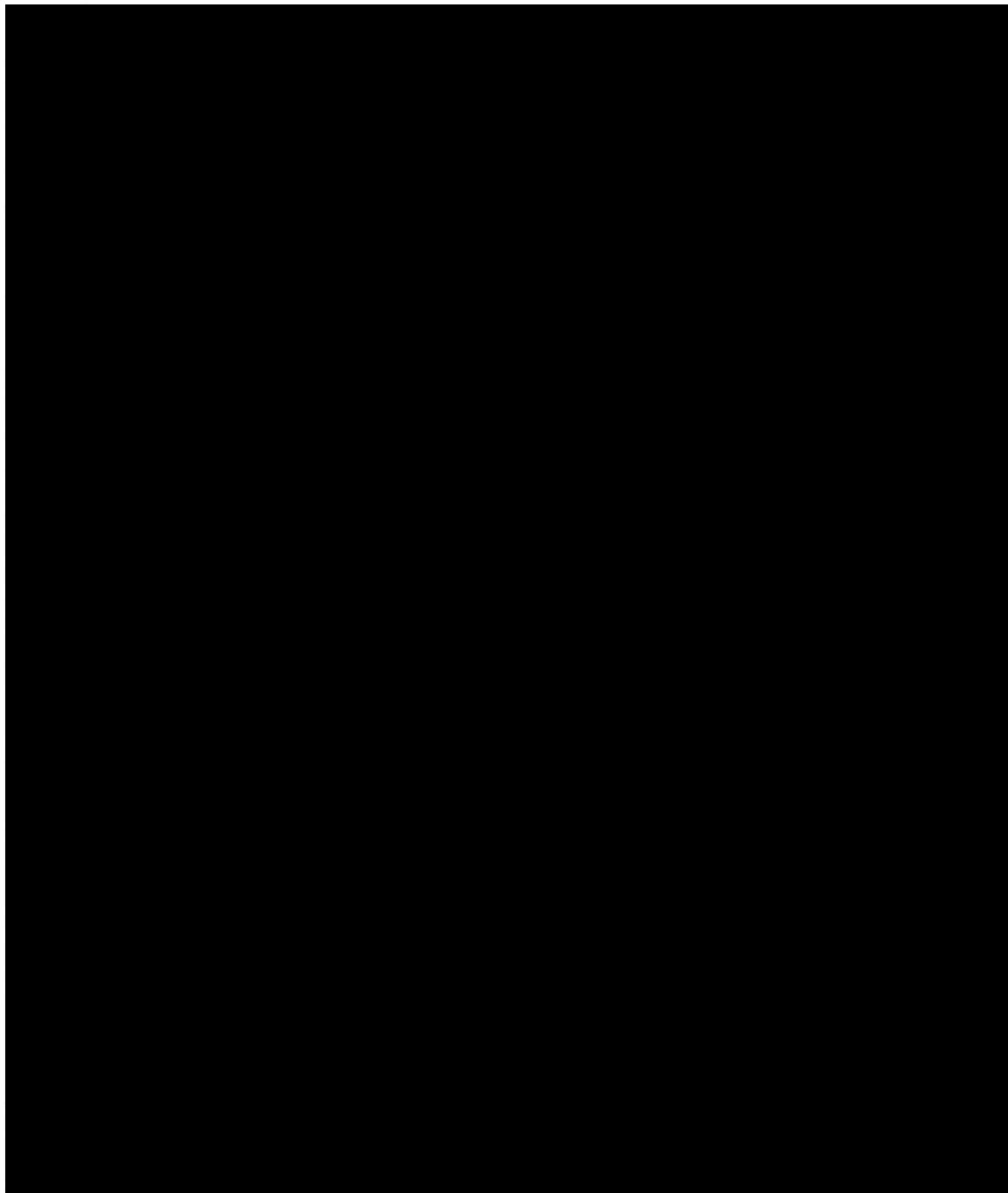






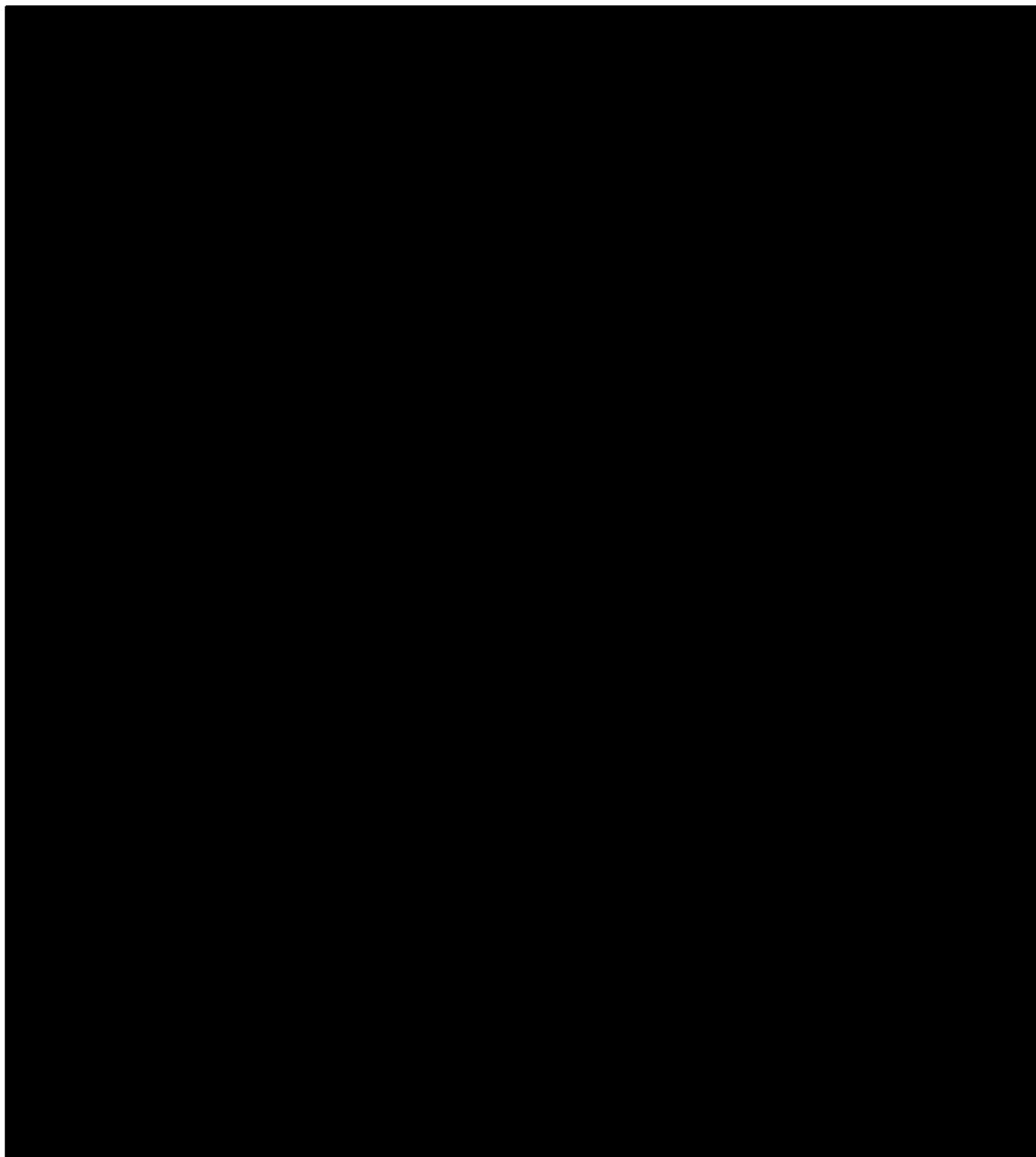


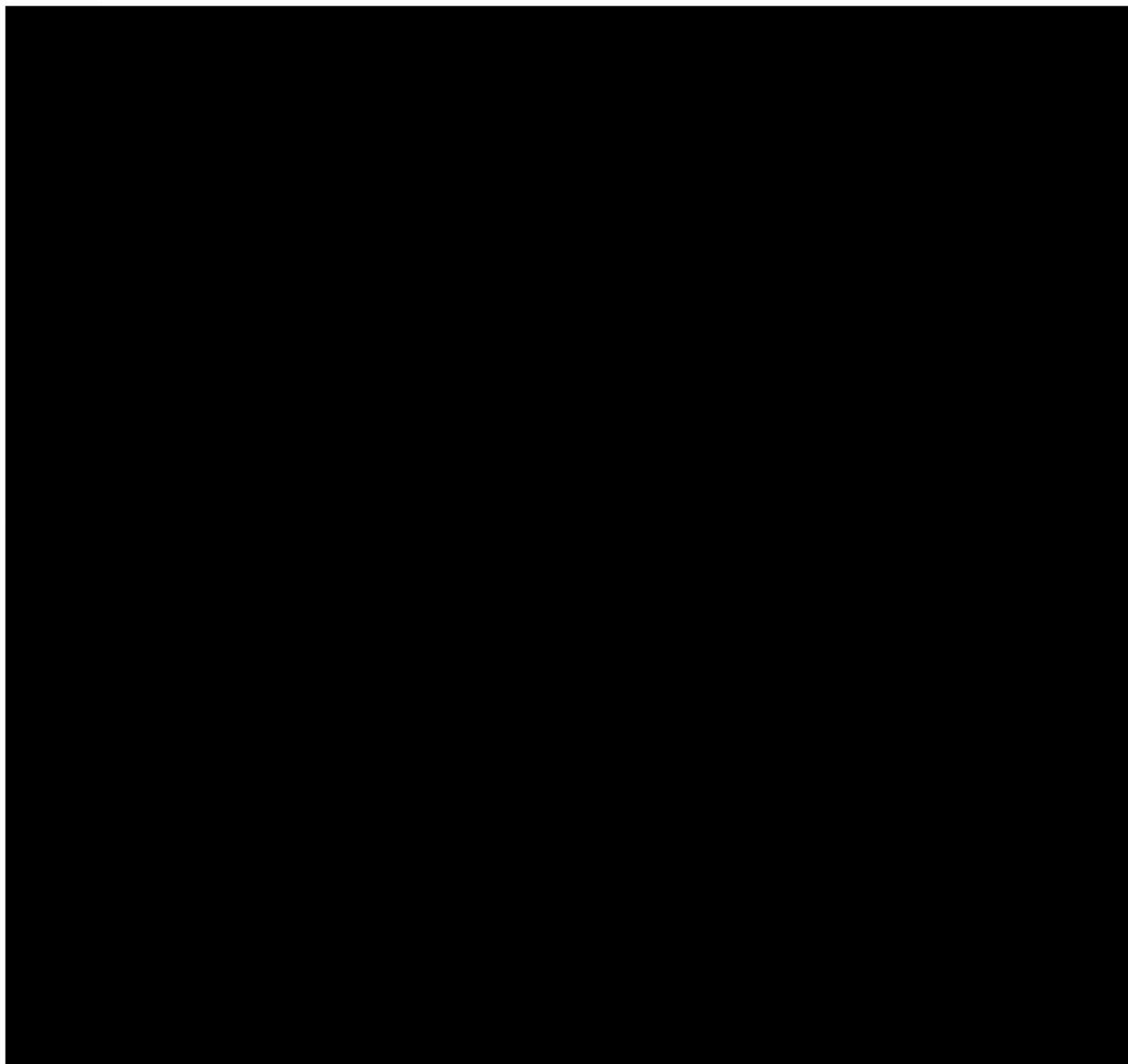




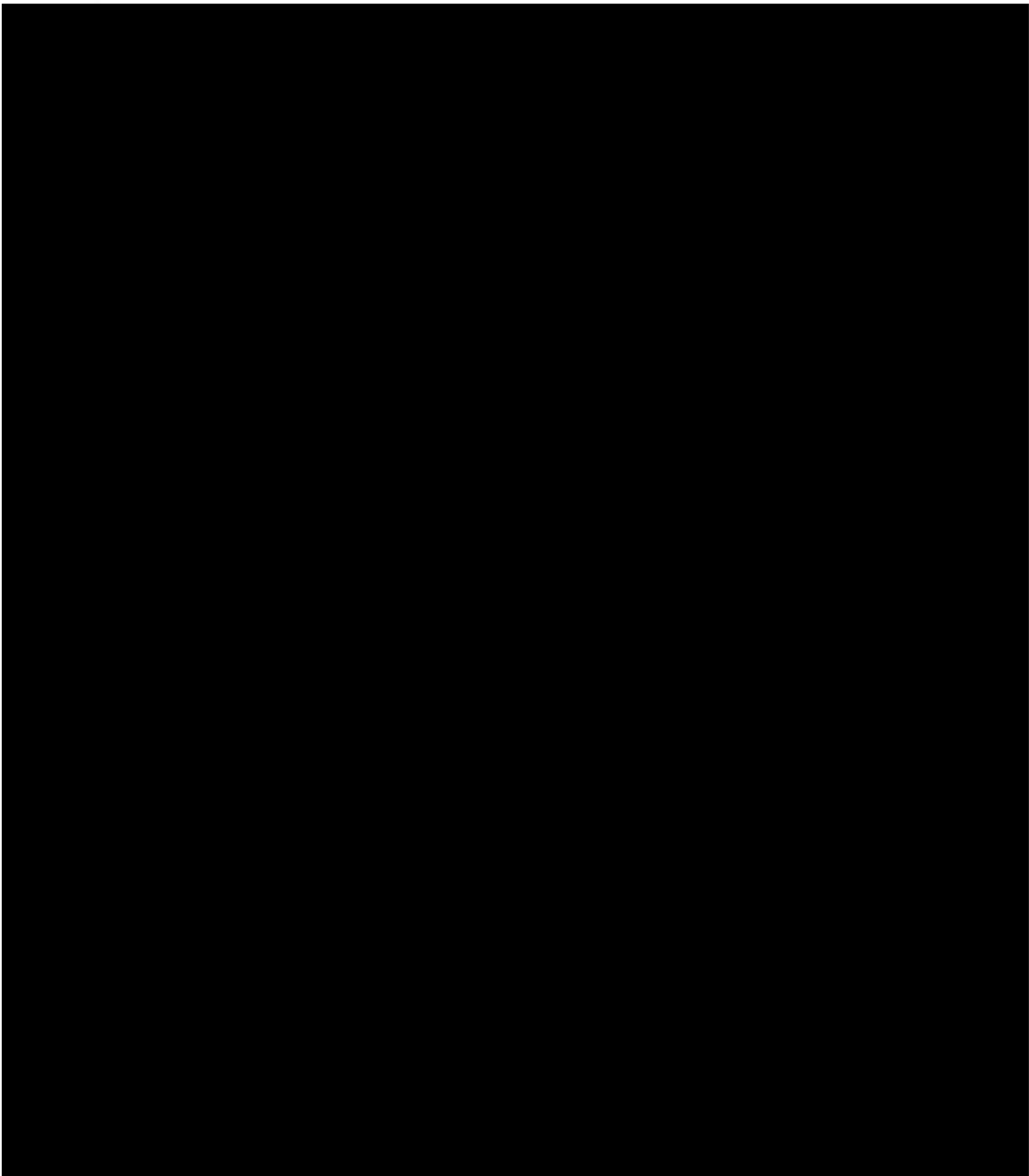


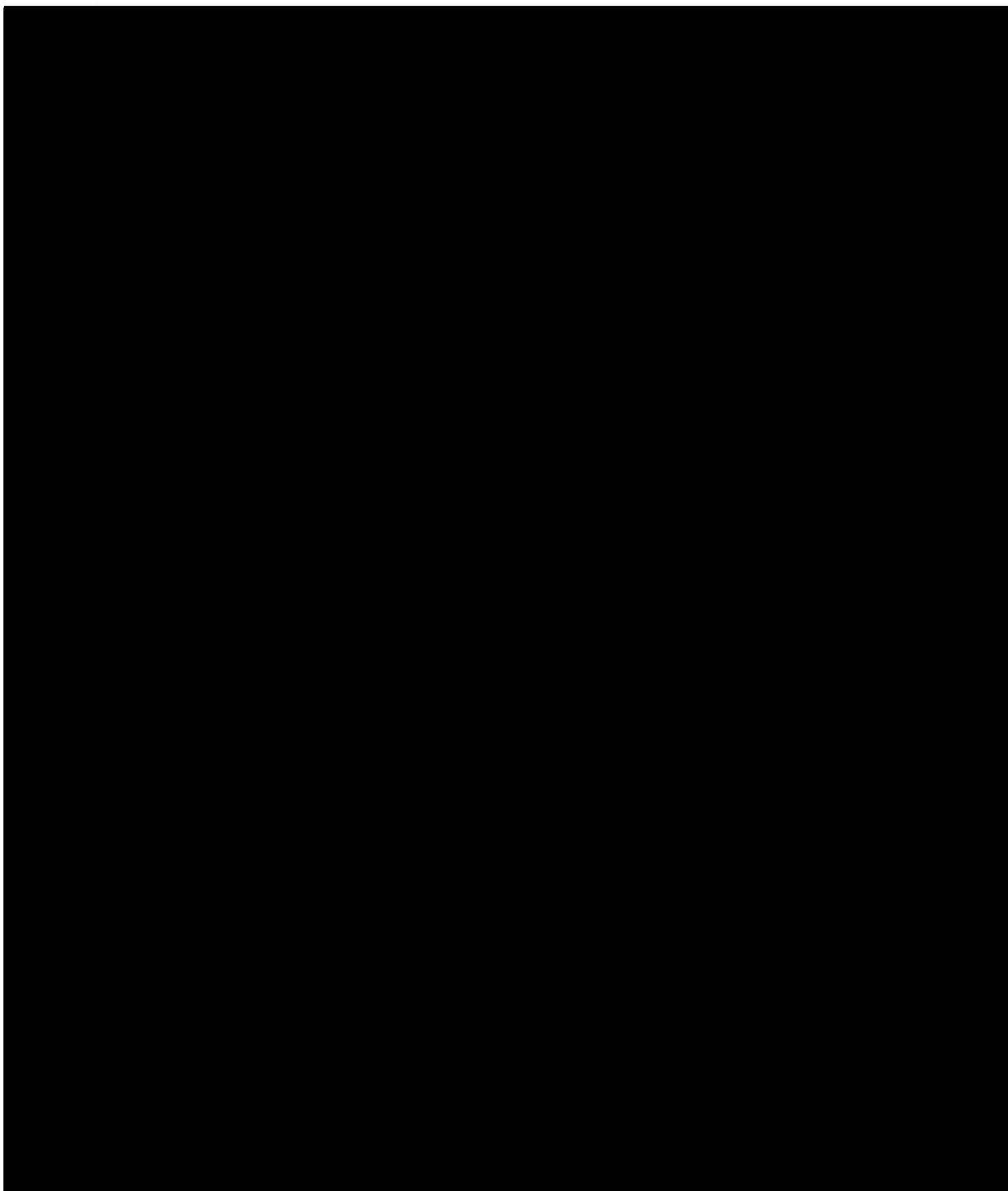


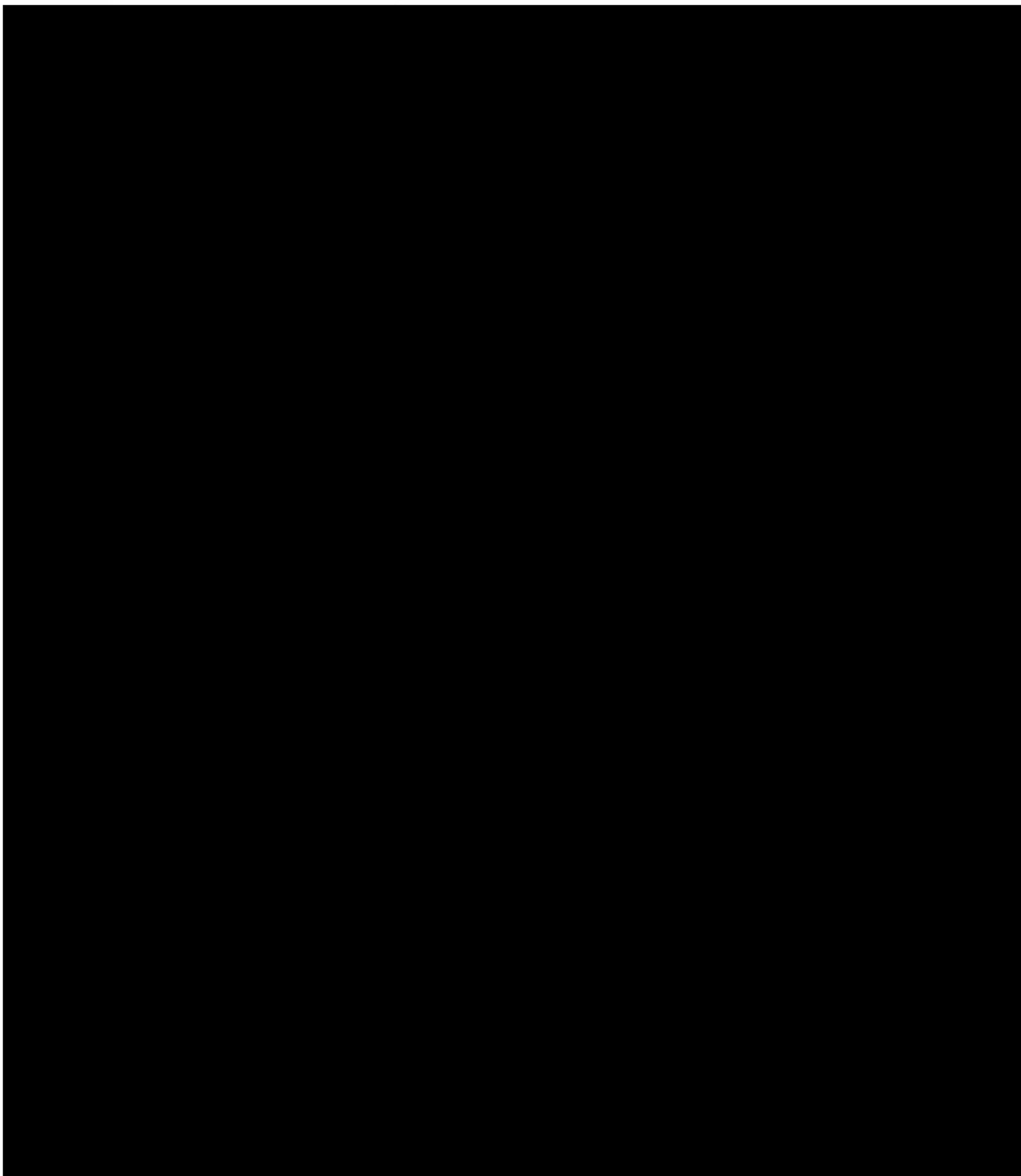


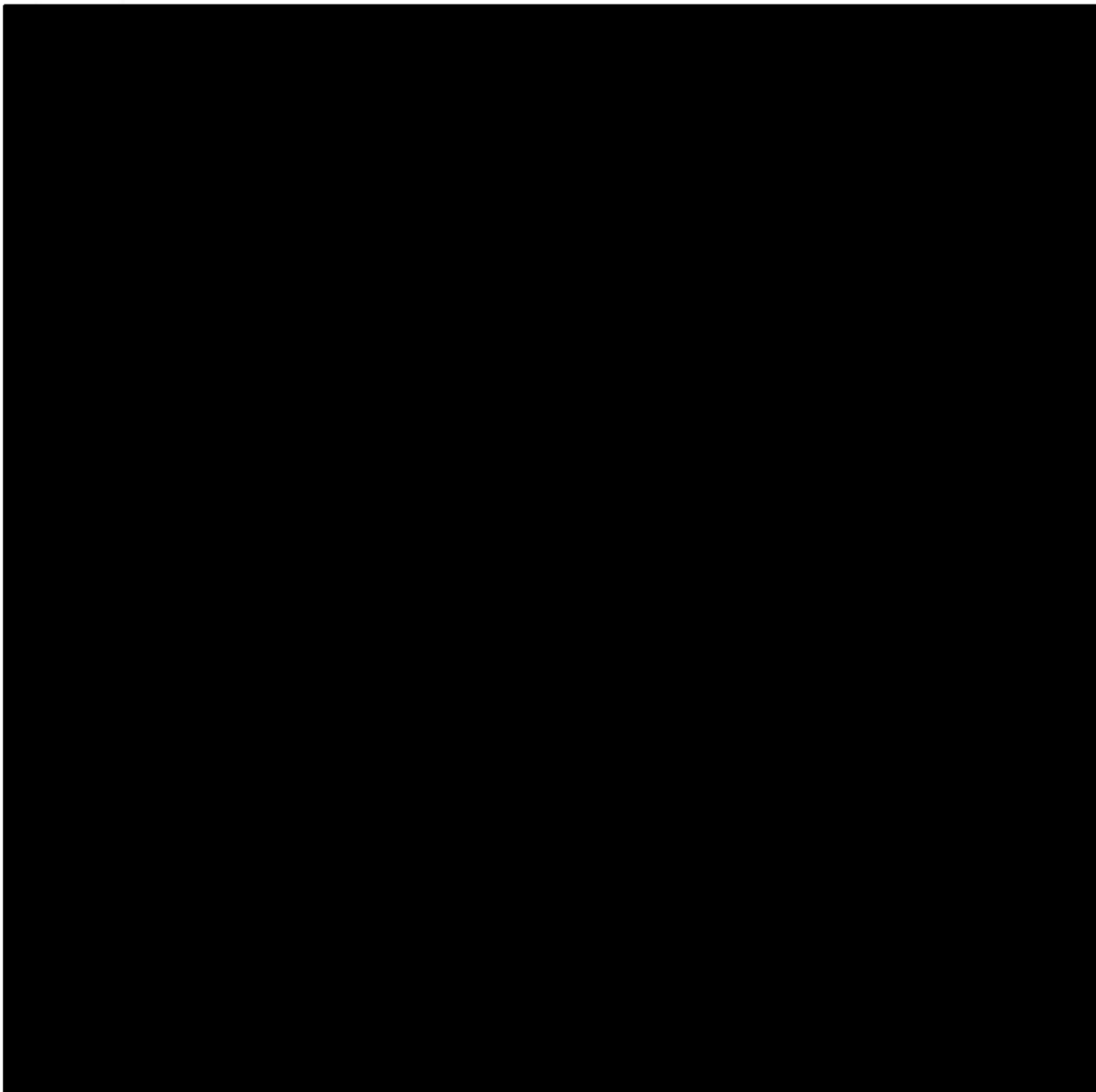


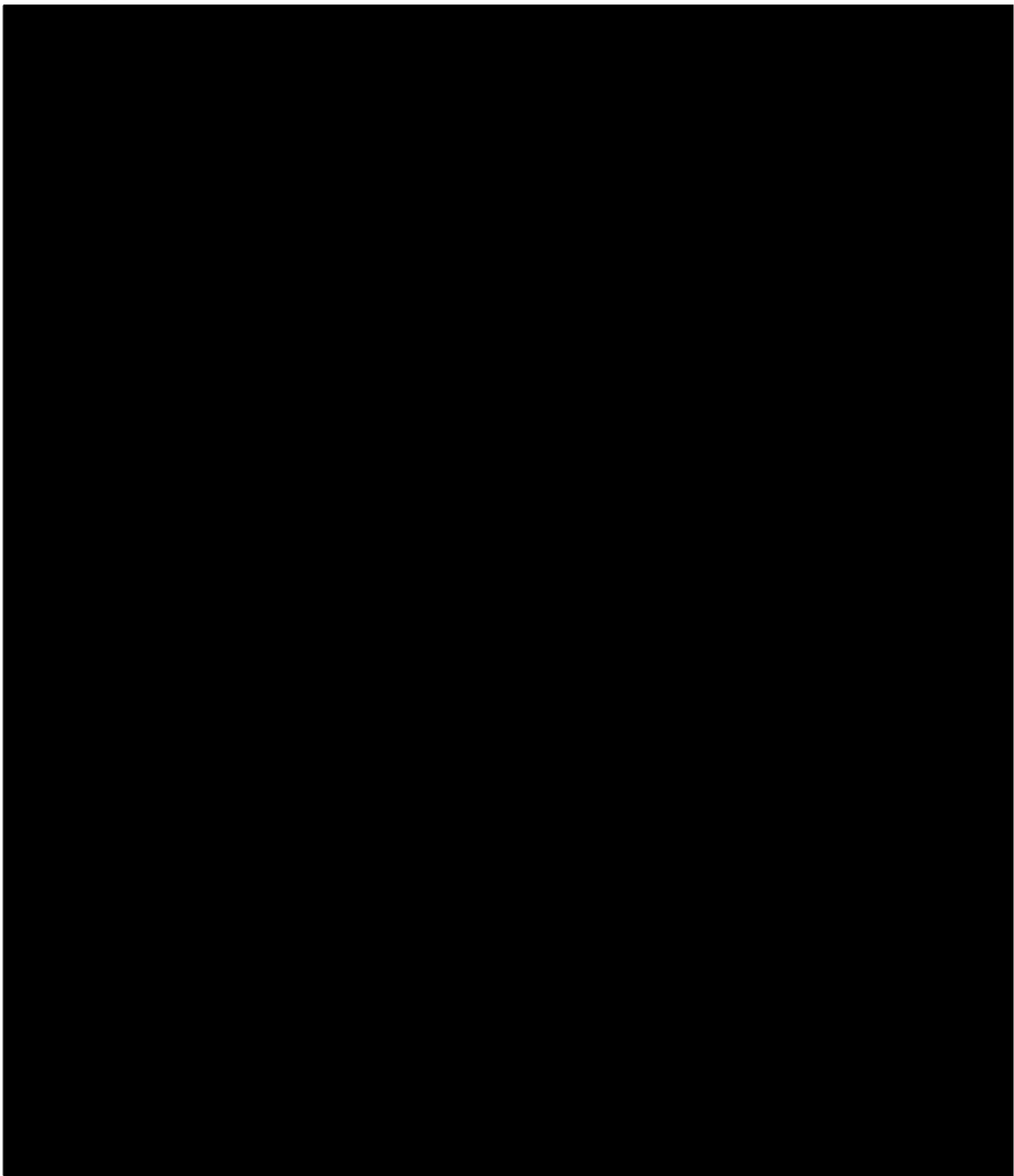


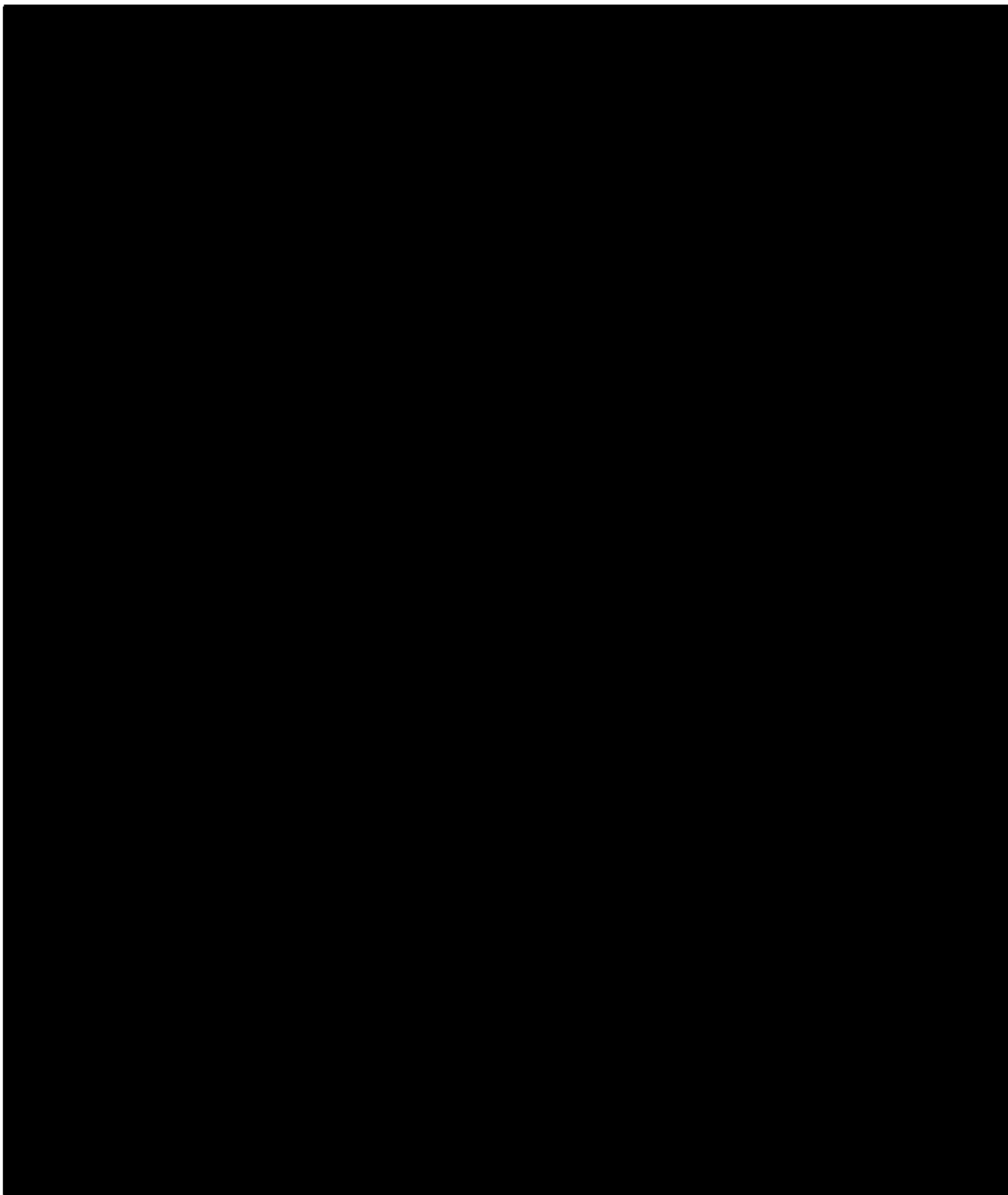


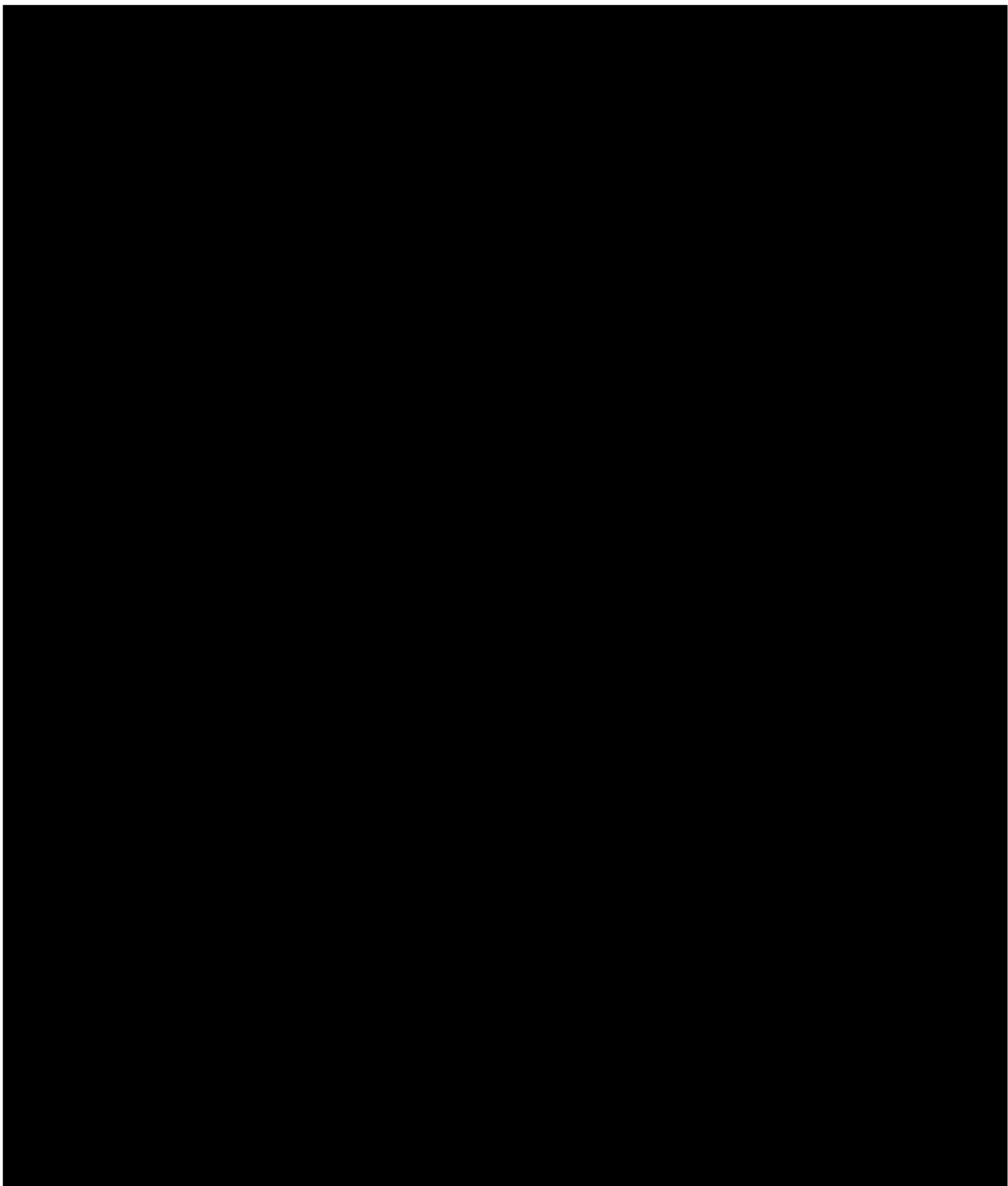


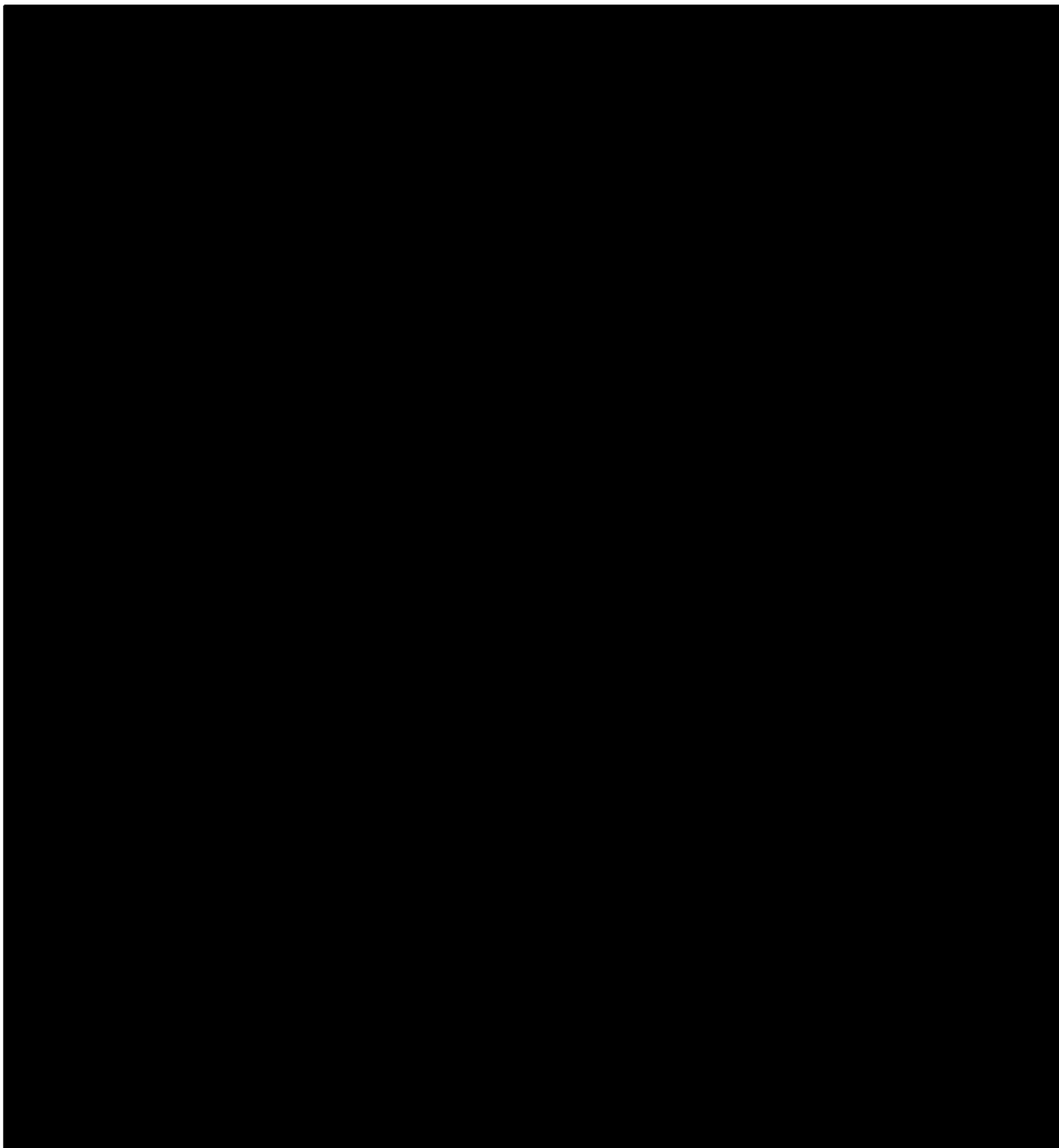




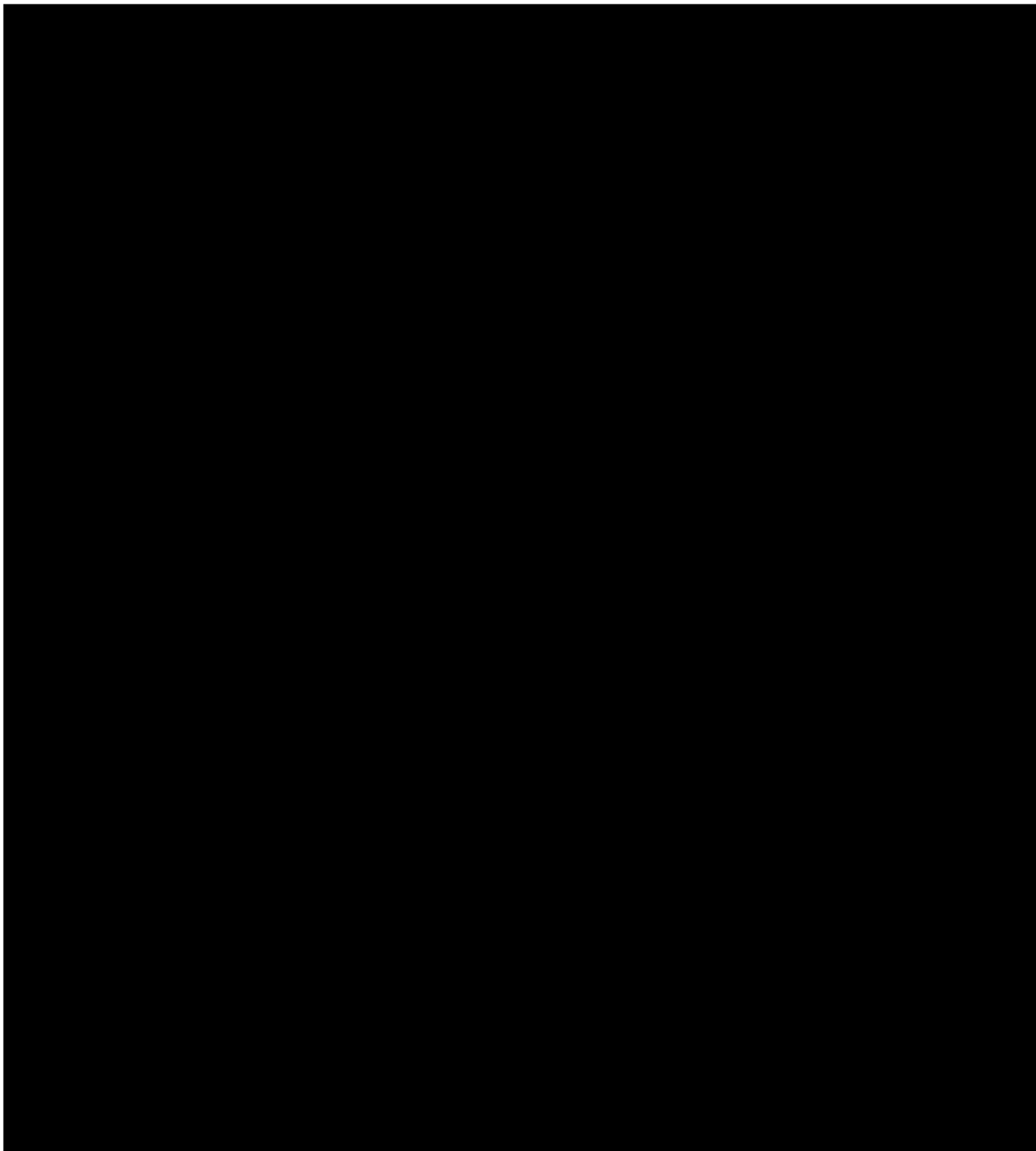












**BACKGROUND CONCERNING GOOGLE**

34. In my training and experience and information conveyed to me from other agents, I have learned that Google provide a variety of on-line services, including electronic mail (“email”) access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com like the accounts listed in Attachment A-1 through A-4. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information, including the subscriber’s full name, physical address, telephone

numbers and other identifiers, alternative email addresses and, for paying subscribers, means and source of payment (including any credit or bank account number). Therefore, the computers of the Google are likely to contain stored electronic communications (including retrieved and unretrieved email for the Providers subscribers) and information concerning subscribers and their use of Google's services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

35. Google's subscribers can also store with the provider files in addition to emails, such as address books, contact, or buddy lists, calendar data, pictures (other than ones attached to emails) and other files on servers maintained and/or owned by the Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

36. Google provides numerous free services to its users with a Google account. Some of these services include Gmail, YouTube, Voice, Blogger, Android, Photos, Drive, Location History, and Search and Browsing History. Gmail is a web-based email service. YouTube is a free video sharing website that allows users upload, view and share videos. Voice is Google's calling, voicemail transcription, and text messaging service. Blogger is Google's free weblog publishing tool for sharing text, photos, and video. Android is Google's open-source operating system used

for mobile devices. Photos stores images for a broad range of Google products. Drive is Google's online storage service for a wide range of file types.

37. In my training and experience, Google typically retains certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

38. In my training and experience, in some cases, account users will communicate directly with Google about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Google typically retains records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user because of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

39. As explained herein, information stored in connection with an account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under

investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts list, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the provider can show how and when the account was accessed or used. For example, as described below, providers typically log the Internet Protocol (IP) addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a time (e.g., location information integrated into an image or video sent via email). Lastly, stored electronic data may provide relevant insight into the account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), actions taken in furtherance of the crime (e.g., researching how to conduct the crimes or communicating with co-conspirators), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement). In my experience, users of these services tend to keep and store communications

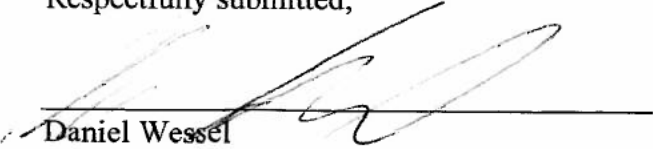
and other information in their accounts well after the completion of such crimes and continue to communicate through these services about their crimes after the crimes have been completed.

**CONCLUSION**

40. Given the above, I believe there is probable cause to believe that the **Target Accounts** contain evidence of violations of 18 U.S.C. §§ 1349 (fraud conspiracy), 1344 (bank fraud), 513(a) (possession of counterfeited or forged securities), and 1028A (aggravated identity theft). Based on the forgoing, I request that the Court issue the proposed search warrant.

41. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

  
\_\_\_\_\_  
Daniel Wessel  
Postal Inspector  
U.S. Postal Inspection Service

THE ABOVE AGENT HAS ATTESTED  
TO THIS AFFIDAVIT PURSUANT TO  
FED. R. CRIM. P. 4.1(b)(2)(B) THIS 27th  
DAY OF JUNE 2023.

  
\_\_\_\_\_  
SONJA F. BIVINS  
UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A-1**

**Property to Be Searched**

This warrant applies to information associated with the Google account [REDACTED]@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

**SEALED**

**ATTACHMENT A-2**

**Property to Be Searched**

This warrant applies to information associated with the Google account [REDACTED]@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.



**ATTACHMENT A-3**

**Property to Be Searched**

This warrant applies to information associated with the Google account [REDACTED]@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

**ATTACHMENT A-4**

**Property to Be Searched**

This warrant applies to information associated with the Google account [REDACTED]@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google LLC and/or Google Payment Corporation (“Google”)**

To the extent that the information described in Attachments A-1 through A-4 is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose to the government for each account or identifier listed in Attachments A-1 through A-4 the following information from **December 11, 2017 to the present**, unless otherwise indicated:

- a. All business records and subscriber information, in any form kept, pertaining to the Account, including:
  1. Names (including subscriber names, user names, and screen names);
  2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
  3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
  4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions, including log-in IP addresses;
  5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
  6. Length of service (including start date and creation IP) and types of service utilized;
  7. Means and source of payment (including any credit card or bank account number); and

**SEALED**

8. Change history.

- b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs;
- d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails. All forwarding or fetching accounts relating to the accounts;
- e. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;
- f. Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;
- g. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.
- h. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, applications, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data and backups; SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record;

any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

- i. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;
- j. All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;
- k. All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history;
- l. All payment and transaction data associated with the account, such as Google Pay and Google Wallet, including: records of purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP address, time stamp, location data, and change history;
- m. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history;



- n. All Google Voice records associated with the account, including: forwarding and other associated telephone numbers, connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history;
- o. The contents of all media associated with the account on YouTube, whether active, deleted, or in draft, including: copies of videos and other media only if uploaded to, saved to, shared by or shared with the account; playlists; connected applications; associated URLs for each record; creation and change history; privacy settings for each record; and all associated logs, including IP addresses, locations, timestamps, and device identifiers; and
- p. Records associated with the account's YouTube registration, including the account's display name, IP logs, channel ID, account registration information, and registration email.

Google is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §§ 1349 (fraud conspiracy), 1344 (bank fraud), 513(a) (possession of counterfeited or forged securities), and 1028A (aggravated identity theft), those violations involving [REDACTED]

[REDACTED] and others, both known and unknown, and occurring after **December 11, 2017**, including, for each Account or identifier listed on Attachments A-1 through A-4, information pertaining to the following matters:

- a. Theft of mail;
- b. Fraudulent deposits of stolen, counterfeited, forged, altered, and/or printed checks, and travel relating thereto;
- c. Use of fraudulent identifications and theft of personal identifying information of victims;

- d. Communications between [REDACTED] and any coconspirators involving theft of mail, fraudulent check deposits, and identity theft, travel in furtherance of the scheme, and preparatory steps taken in furtherance of the scheme;
- e. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- f. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;
- g. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).
- h. The identity of the person(s) who communicated with the Account about matters relating to mail theft, fraudulent check deposits, and identity theft, including records that help reveal their whereabouts.